C. Remarks

Claims 7 through 36 are currently pending. Claims 1 through 6 have been cancelled.

Objections to the Claims

Claims 2 and 16 were objected to under 37 C.F.R. §1.75(c). Inasmuch as that subsection only concerns multiple dependent claims, Applicants' Attorney believes that the objection was intended to be made under 37 C.F.R. §1.75(b) and M.P.E.P. §706.03(k). If this is an incorrect assumption, Applicants' Attorney requests clarification of the basis for objection.

Claim 2 has been cancelled. Relative to Claim 16, the Action asserts, in support of the objection, that Claims 12 through 15 have already defined a proxy system. Thus, the additional specific limitation to a proxy recited in Claim 16 provides no substantive differentiation.

The asserted reading of Claims 12 through 15 is, however, not correct when considered in the relevant context. That is, in a completely abstract context, any intermediary transferring information between two endpoints may be considered a proxy. In the specific context to which the present invention – and claims – pertains, "proxy" operation defines a specific nature of representing the source identity of network data. Claims 12 through 15 are properly read as not requiring the network storage controller itself to substitute as the source identity relative to the data stores, *i.e.*, operate as a proxy. Claim 16, however, specifically requires the network storage controller to operate as a proxy, thereby concealing the source identity of the network data as being the client computers at least as represented in the visible network data packets.

Therefore, Claim 16 presents a substantive claim distinction more than sufficient to overcome any reasonably valid objection under 37 C.F.R. §1.75(b). Applicants' Attorney respectfully requests withdrawal of the objection against Claim 16.

Rejections under 35 U.S.C. §102 – the Lin Reference:

Claims 1-9, 12-17,19-22, and 24-34 were rejected under 35 U.S.C. §102(b) in view of Lin et al (US Patent 6,052,785).

In order to establish a rejection under 35 U.S.C. §102, all elements of a claim must be identically found in a prior art reference. See, M.P.E.P. §706.02 (For anticipation under 35 U.S.C. 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present) (emphasis added); M.P.E.P. §2112 (In relying upon the theory of inherency, the Examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art. Ex parte Levy, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis in original); M.P.E.P. §2131.

The essential nature of anticipatory identity requires that the function of the elements and their interconnections not just be colorably similar, but identical in all aspects (emphasis added). See, Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) (The identical invention must be shown [by the reference] in as complete detail as is contained in the ... claim). Clearly, a prior art reference that discloses a collection of elements that are assembled differently and that function collectively in a different or incomplete way compared to the claimed invention is not an anticipating reference.

In the present case, the Lin reference describes a system that operates in a completely different manner to address a completely different problem than that solved by the present claimed invention. The Lin reference describes a three-tier computing system where the middle tier provides for the retention of security information that can be used in establishing secure sessions between the different computer tiers. The problem sought to be solved by the Lin reference is to minimize repeatedly determining security authorizations to ease the burden of establishing secure socket layer (SSL) sessions.

> A security mechanism according to the present invention provides login coordination. This enables the client to authenticate once with the security server and have those credentials used repeatedly without validation. A single security server supporting multiple applications gives the client authenticated access to those multiple applications without the overhead of repeated credential requests and validations. This increases the responsiveness and throughput of the server. (Column 8, ll. 10 - 18.)

Client SSL sessions with the middle tier are terminated at the middle tier. As best can be understood from the Lin reference, no secure session is established between the middle tier with the back-end tier. As taught, the back-end tier provides for the mounting of file-system devices on the middle tier server for access from client tier users. Security of the data transferred between the middle and back-end tiers is simply not addressed in the Lin reference.

In contrast, the present invention, as claimed, is directed to securing "media-level data." The term "media-level data" is defined in the present application as referring to the file data transported within select network data packets between a network storage access controller and typically back-end storage systems:

> ... The primary function of the network media access controller 14 is to provide storage security for client data stored by the

> iSCSI targets 20. The network media access controller 14 preferably operates to encrypt the media-level data contained in selected iSCSI network data packets directed to any of the iSCSI targets 20 and correspondingly decrypt the media-level data in returned iSCSI data packets. In accordance with the present invention, media-level data is the SCSI data payload within an iSCSI network data packet. The presence of such media-level data is preferably identified by examination of the SCSI command or command response embedded within a corresponding iSCSI network data packet. (¶54; Emphasis added.)

The present invention, as claimed, requires the selective encryption processing of media-level data distinct from other portions of a network data packet.

Claim 7: c) a controller coupled between said first and second network interfaces operative to convert between said first and second network data, said controller including a crypto processor to encrypt and decrypt media-level storage data contained in said first and second network data. (Emphasis added.)

Claim 12: wherein said network data includes media-level data and wherein said network access controller provides for the selective encryption and decryption of said media-level data transferred with respect to said plurality of data stores. (Emphasis added.)

Claim 17: a network data processor coupleable between an initiator network and a target network to provide for the proxy transfer of predetermined network protocol data packets containing media-level data between said initiator and target networks, said network data processor being operative to selectively process said predetermined network protocol data packets to encrypt and decrypt media-level data. (Emphasis added.)

Claim 24: a) first processing ... to identify predetermined network data packets containing media-level data; and
b) second processing ... to encrypt ... and to decrypt the media-level data contained in said predetermined network data packets being transferred ... . (Emphasis added.)

Claim 28: b) crypto processing, on passage through said network storage portal, media-level data contained within network storage data packets to selectively encrypt, at said network storage portal, media-level data passed to said network data store and selectively decrypt, at said network storage portal, media-level data passed from said network data store. (Emphasis added.)

Claim 34: a network data processor ... using a data transfer protocol encapsulated by a network communications protocol, wherein said data transfer protocol provides for the storage and retrieval of media-level data, wherein said network data processor is operative to transfer network data packets conforming to said network communications protocol between said initiator and target network interfaces, said network data processor being further operative to selectively encrypt and decrypt media-level data contained within network data packets transferred between said initiator and target network interfaces. (Emphasis added.)

The Lin reference teaches SSL-type client session encryption of entire network data packets regardless of the nature or data content of the data packets begin transferred. Moreover, as between the middle and back-end tiers, the Lin reference does not literally teach the use of encrypted network data transfers directly with respect to a storage system.

Given that the Lin reference teaches completely undifferentiated encryption of network packets, the reference does not identically teach the invention as claimed in the pending independent Claims 7, 12, 17, 24, 28 or 34, as established above, or the dependent claims. Accordingly, Applicants' respectfully request reconsideration of the rejection of Claims 7, 12-17,19-22, and 24-34.

Rejections under 35 U.S.C. §102 – the Berger Reference:

Claims 1-36 were also rejected under 35 U.S.C. §102(b) in view of Berger et al (US Patent 5,850,446).

The Berger reference, like the Lin reference, describes a system that is directed at solving a fundamentally different problem. The Berger reference describes a secure electronic transaction (SET) system. Client/merchant systems submit SET requests to a gateway system for authentication and payment. Figure 4 and the text at column 15, ln 68 through column 17, ln 8 detail the construction of a SET request. Notably, this includes the compilation of a pre-encrypted certificate, securely identifying the merchant, into the SET request. The request itself is encrypted using a key that is then envelope encrypted and packed into the SET request.

Clearly, nothing in a SET request is or even remotely corresponds to "media-level data."

The gateway system, in element 2120 of Figure 21a performs the process shown in Figures 6a and 6b, which is described at column 17, ll. 10-61. In summary, the gateway system, parses the SET request to authenticate the merchant and process the request. Various details determined through the processing of the request result in queries directed to other systems and, in some cases, the saving of data to databases on disk. Nowhere does the Berger reference teach or suggest that any encrypted data be stored to disk – at least Applicants' Attorney could find no such description; the few citations provided in the Action in support of the rejection were checked, but were not found relevant.

Finally, the gateway system provides a response to a SET request by creating a network message analogous to the SET request. That is, the response as a whole is encrypted and packaged with an envelope encrypted key for transfer back to the client/merchant.

The Berger reference thus provides no teaching of the selective encryption of media-level data that is then transferred over a network for storage. As with the Lin reference, the

reference teaches the need for security and the implementation of encryption with respect to the client, not the data storage tier.

As established above, the present invention as set forth in the pending claims calls for the selective encryption of "media-level data" that is then transferred for storage and the decryption of "media-level data" that is retrieved from storage. Such is not identically taught by the Berger reference.

Accordingly, Applicants' respectfully request reconsideration of the rejection of pending independent Claims 7, 12, 17, 24, 28 or 34 and the claims dependent therefrom.

Rejections under 35 U.S.C. §103:

Claims not identically shown by a reference otherwise available under 35 U.S.C. §102(a), (b), or (e) may be obvious under 35 U.S.C. §103. To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See also, M.P.E.P. §§2142, 2143.

No rejections under 35 U.S.C. §103 and arguments in support thereof have been presented by the Examiner in the alternative to the rejections under 35 U.S.C. §102. Consequently, no legally sufficient prima facie case of obviousness has been made against the pending claims. Purely for purposes of advancing the consideration of the claims, however, Applicants' Attorney provides the following comments regarding any potential

assertion of obviousness based on the Lin and Berger references with respect to the pending claims.

As established above, both of the cited references are directed to systems intended to solve entirely different problems than addressed in the present application. The Lin reference is focused on improving the security and efficiency of providing network access to mounted storage devices as presented on a middle tier system. Security of file data in transport between the middle and back-end tiers and as stored on the back-end tier is simply presumed. Thus, the Lin reference presents no motivation, let alone some actual suggestion, to even consider securing any stored data. The Berger reference similarly fails to be concerned with the secure storage of data.

The references certainly provides no motivation or suggestion to do what Applicant teaches as set forth in the pending claims.

Accordingly, the presently pending claims are not obvious in view of the Lin and Berger references, alone or in any combination.

Conclusion:

In view of the above Amendments and Remarks, Applicants respectfully assert that Claims 7-36 are now properly in condition for allowance. The Examiner is respectfully requested to take action consistent therewith and pass this application on to issuance. The

Examiner is respectfully requested to contact the Applicants' Attorney, at the telephone number provided below, in regard to any matter that the Examiner may identify that might be resolved through a teleconference with the Examiner.

Respectfully submitted,

Date: 1/25/2006

By: Gerald B. Rosenberg

Gerald B. Rosenberg
Reg. No. 30,320

NEWTECHLAW
285 Hamilton Avenue, Suite 520
Palo Alto, California 94301
Telephone: 650.325.2100